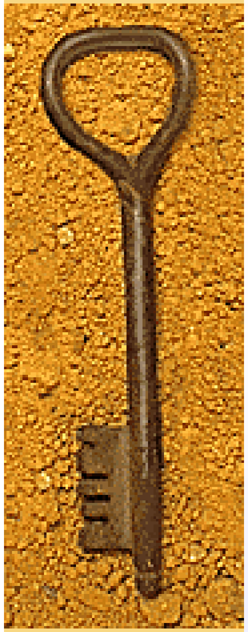
Aesec

Security Requirements for Operating Systems

A View from 30 Years Experience

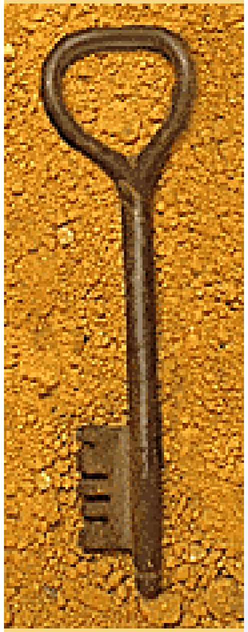
Dr. Roger R. Schell
schellr@acm.org



Integrating Multiple Perspectives

- Creation of Reference Monitor Concept
- Secure (Class B2) Multics Time Sharing
- Comm Processor (Class A1) Architecture
- 1st Widely Used Security Standard
  - TCSEC (“Orange Book”)
- High Assurance (Class A1) COTS Product
- Market Leading Network O/S (Class C2)
- Global High Value B2B E-Commerce Needs

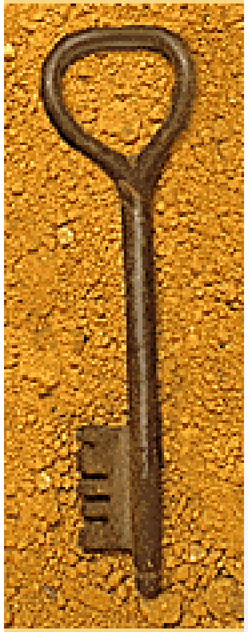
Aesec



Gemini Class A1 Security Kernel

- Built to Clear Security Requirements
  - 9 Concise Pages of Well Formed Criteria
- Practicality of Evaluations and Technology
  - Small Startup Successfully Evaluated Product
  - Always Clear What Counted for Success
- Contrary to Myths, Short Evaluation Period
  - Prompt Evaluation After Product Completion
- Adequate for Most Demanding Security
  - Blacker Class A1 “VPN”
  - Most Sensitive Military and Diplomatic Data
- Hard to Compete Against Gov’t (e.g., MISSI)

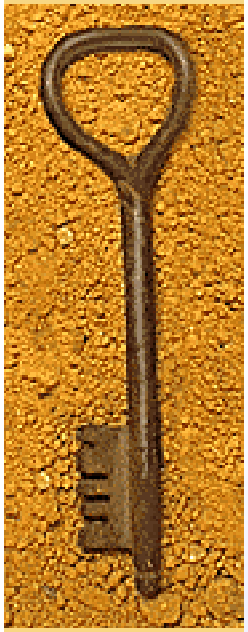
Novell Class C2 Network



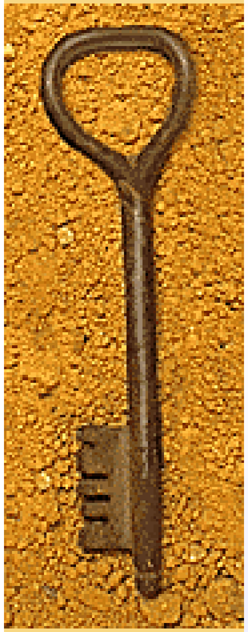
- First Full Network Evaluation (TNI)
  - Separate Evaluated Client Component
  - Separate Evaluated Servers
  - Evaluated Network Security Architecture
- Practical Flagship Product Currency
  - Novell “YES” for New Hardware
  - Practical RAMP of Commercial Product
- Parallel European ITSEC Evaluation Evidence
- C2 Requirements Easily Assimilated
  - Commercial Development Environment
  - Not Experienced Security Experts
- Business Case Based on Well-known Ratings

Aesec

Weak CC Business Case

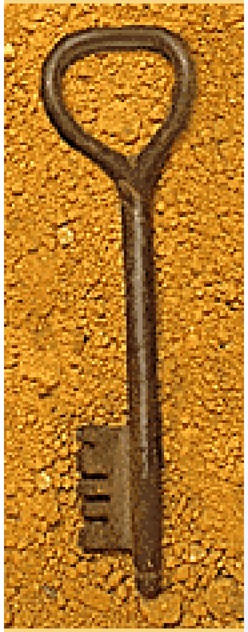


- Lack of Ordered Comparable Levels
  - Extraordinary Influence By Dominant Vendors
  - Weak Basis for Competitive Business Case
  - No Means for Practical High Assurance Evaluations
- Lacks Incremental Evaluations
  - Separate Network Components (e.g., TNI)
  - Separate Application Components (e.g., DBMS)
  - Policy Components (i.e., Balanced Assurance)
- Lacks Practical Product Currency
  - Ratings Maintenance Program (RAMP)
  - Platform Independence (e.g., Novell “YES”)
- Lacks Link to Systems **Security** Foundation



Value of High Assurance

- Growing Threat and Security Need
- Value of 3rd Party Evaluation
  - Greatest for Highest Value and Risk
  - Requires High Assurance Evaluations (e.g., A1)
  - Must Address Trap Doors and Trojan Horses
- Customers Can’t Evaluate for Themselves
  - Expertise Needed, Especially At High Assurance
  - Vendors Also Unwilling to Expose Designs Details
- It is Customers Who Face Risk and Liability
  - Cannot Evaluate for Themselves
  - Can Apply Objective Third Party Evaluation
  - But Need Criteria Responsive to Risk



Conclusions

- Adequate Technology Exists
  - Highly Secure Kernelized Operating Systems
  - Highly Reliable (Class A1) Evaluations
- Growing Demands to Protect High Value
  - Military and Diplomatic (Historical Need)
  - Business-to-Business E-Commerce
  - Regulatory (e.g., Privacy and Financial)
- Government Has Abandoned Leadership
  - Evaluation Not Available to Emerging Innovators
  - Discontinued Class A1 Evaluations
  - Avoidance of Mandates (e.g., “C2 by ’92”)
- Lack of Will to Use Available Technology
  - There is No Free Lunch